

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007214

(43)Date of publication of application : 11.01.2002

(51)Int.Cl. G06F 12/14
G06F 1/00

(21)Application number : 2000-192757 (71)Applicant : TOSHIBA CORP

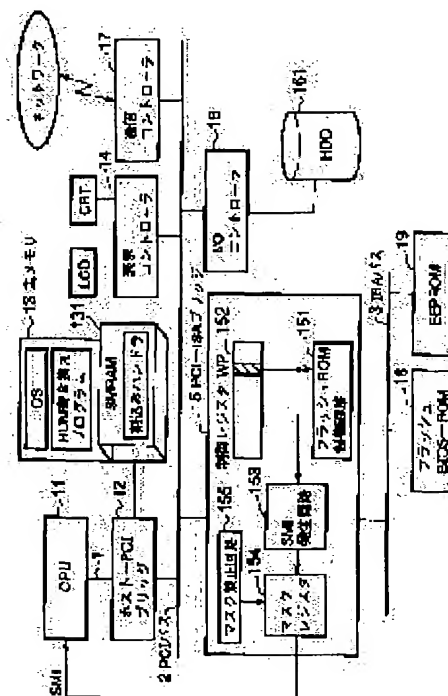
(22)Date of filing : 27.06.2000 (72)Inventor : MAEDA MAYUMI

(54) INFORMATION PROCESSOR AND REWRITE CONTROL METHOD OF NONVOLATILE STORAGE DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve security level by stopping a nonvolatile storage device from being rewritten in unauthorized manner by software.

SOLUTION: A ROM rewriting program performs access for rewriting a write protect bit WP in a control register 152 to '1' in a series of ROM rewrite processes and releases the write protect of a flash BIOS-ROM 18. At this time, an SMI-generating circuit 153 issues an SMI signal to a CPU 11. In response to this SMI signal, an interrupt handler is actuated. The interrupt handler authenticates whether the access by the ROM rewriting program is authorized, and performs access for rewriting the write protect bit WP in a control register 152 to '0' and re-sets the write protect of the flash BIOS-ROM 18, and stops the rewriting when deciding that the access is not authorized.



LEGAL STATUS

[Date of request for examination] 27.06.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other
than the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-7214

(P2002-7214A)

(43) 公開日 平成14年1月11日 (2002.1.11)

(51) Int.Cl.⁷

識別記号

F I

テーマコード(参考)

G 0 6 F 12/14
1/00

3 1 0

G 0 6 F 12/14
9/06

3 1 0 K 5 B 0 1 7
6 6 0 J 5 B 0 7 6

審査請求 有 請求項の数10 O L (全 9 頁)

(21) 出願番号

特願2000-192757(P2000-192757)

(22) 出願日

平成12年6月27日(2000.6.27)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 前田 真弓

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B017 AA02 BA04 BB00 CA12

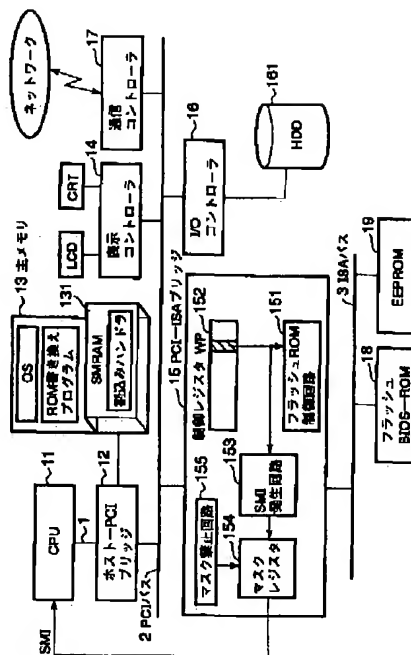
5B076 FB02

(54) 【発明の名称】 情報処理装置および不揮発性記憶装置の書き換え制御方法

(57) 【要約】

【課題】ソフトウェアによる不揮発性記憶装置の不正な書き換えを阻止できるようにし、セキュリティレベルの向上を図る。

【解決手段】ROM書き換えプログラムは、一連のROM書き換え処理の中で、制御レジスタ152内のライトプロテクトビットWPを“1”に書き換えるアクセスを実行し、フラッシュBIOS-ROM18のライトプロテクトを解除する。このとき、SMI発生回路153からCPU11にSMI信号が発行される。このSMI信号に応答して、割り込みハンドラが起動される。割り込みハンドラは、ROM書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い、正当なアクセスではないと判定した場合には、書き換えを阻止するために、制御レジスタ152内のライトプロテクトビットWPを“0”に書き換えるアクセスを実行し、フラッシュBIOS-ROM18のライトプロテクトを再設定する。



【特許請求の範囲】

【請求項1】 不揮発性記憶装置の記憶内容を書き換え可能な情報処理装置であって、

CPUと、
前記不揮発性記憶装置の書き換えに必要な所定のハードウェアに対する、ソフトウェアからのアクセスにตอบสนองして、前記CPUに割り込み信号を発生する割り込み信号発生手段と、

前記割り込み信号発生手段からの割り込み信号の発生を契機に前記CPUによって起動され、前記ソフトウェアによるアクセスが不当なものである場合、前記不揮発性記憶装置の書き換えを禁止する書き換え制御手段とを具備することを特徴とする情報処理装置。

【請求項2】 前記書き換え制御手段は、
前記ハードウェアに対するアクセスに先立って実行すべき所定の手順が前記ソフトウェアによってすでに実行されているか否かを判別する手段を含み、その判別結果に応じて前記ソフトウェアによるアクセスが不当なものであるか否かを検出することを特徴とする請求項1記載の情報処理装置。

【請求項3】 前記割り込み信号のマスクを禁止するためのマスク禁止手段をさらに具備することを特徴とする請求項1記載の情報処理装置。

【請求項4】 前記不揮発性記憶装置の書き換えを禁止するためのライトプロテクト機能を有し、前記ライトプロテクト機能の設定が解除されている場合、ソフトウェアからのアクセスにตอบสนองして前記不揮発性記憶装置の書き換えに必要な動作を実行するアクセス制御手段をさらに具備し、
前記割り込み信号発生手段は、前記アクセス制御手段に対してライトプロテクトを解除するためのアクセスがソフトウェアによって行われたとき、それにตอบสนองして前記割り込み信号を発生することを特徴とする請求項1記載の情報処理装置。

【請求項5】 前記書き換え制御手段は、前記ソフトウェアによる前記ライトプロテクトを解除するためのアクセスが不当なものである場合、前記ソフトウェアによる前記不揮発性記憶装置の書き換えを阻害するために前記アクセス制御手段をアクセスして、ライトプロテクトを再設定する手段を含むことを特徴とする請求項4記載の情報処理装置。

【請求項6】 前記書き換え制御手段は、前記ソフトウェアによるアクセスが不当なものである場合、前記ソフトウェアによる前記不揮発性記憶装置の書き換えを阻害するために前記情報処理装置をシャットダウンする手段を含むことを特徴とする請求項1記載の情報処理装置。

【請求項7】 前記不揮発性記憶装置には、前記情報処理装置のハードウェア制御のためのBIOSプログラムが格納されていることを特徴とする請求項1記載の情報処理装置。

【請求項8】 不揮発性メモリに格納されているBIOSプログラムをオペレーティングシステムの動作環境下で書き換え可能な情報処理装置であって、

CPUと、
前記不揮発性メモリの書き換え動作を実行するアクセス制御手段と、

前記オペレーティングシステム上で動作するソフトウェアからの前記アクセス制御手段に対する所定のアクセスにตอบสนองして、前記CPUに割り込み信号を発生する割り込み信号発生手段とを具備し、

前記CPUは、前記割り込み信号によって割り込み処理を実行し、その割り込み処理の中で、前記ソフトウェアによる前記アクセス制御手段に対するアクセスが不当なものであるか否かを検出し、不当なものである場合、前記不揮発性メモリの書き換えを禁止するための処理を行うことを特徴とする情報処理装置。

【請求項9】 情報処理装置内で使用される不揮発性記憶装置の記憶内容の書き換えを制御するための書き換え制御方法であって、

前記情報処理装置内のCPUによって実行されるソフトウェアが前記不揮発性記憶装置の書き換えに必要な前記情報処理装置内の所定のハードウェアにアクセスしたとき、そのアクセスにตอบสนองして前記CPUに割り込み信号を発生するステップと、

前記割り込み信号の発生を契機に前記CPUによって起動される割り込み処理の中で、前記ソフトウェアによるアクセスが不当なものであるか否かを検出し、不当なものである場合、前記不揮発性記憶装置の書き換えを禁止するための処理を実行するステップとを具備することを特徴とする書き換え制御方法。

【請求項10】 前記不揮発性記憶装置には、前記情報処理装置のハードウェア制御のためのBIOSプログラムが格納されていることを特徴とする請求項9記載の書き換え制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はパーソナルコンピュータなどの情報処理装置およびその情報処理装置で使用される不揮発性記憶装置の書き換え制御方法に関する。

【0002】

【従来の技術】近年、携行が容易でバッテリーにより動作可能なノートブックタイプのパーソナルコンピュータ（PC）が種々開発されている。この種のPCに於いては、BIOS（Basic Input Output System）を新しいバージョンにアップグレードするというBIOSアップデートを行えるようにするために、BIOSはフラッシュメモリなどの電氣的に書き換え可能な不揮発性メモリに格納されている。

【0003】BIOSの更新は、通常は、更新用の新たなBIOSファイルおよびBIOS更新用システムプロ

グラムを収めたフロッピー（登録商標）ディスク（FD）をPCに装填した状態でPCをパワーオンし、FDからBIOS更新用システムプログラムを起動することによって行われる。また、最近では、オペレーティングシステムの動作環境下で動作する専用のアプリケーションを実行することによって、BIOSの更新を行う方法も考えられている。この方法により、FDからシステムを起動する必要が無くなるので、フロッピーディスクドライブ（FDD）が装備されていない、いわゆるFDDレスのPCにおいても、容易にBIOSをアップデートすることが可能となる。

【0004】BIOS更新のための不揮発性メモリの書き換え手順はPCのプラットフォーム毎に個々に規定されるものではあるが、その書き換え手順は基本的には公開されている場合が多い。このため、その書き換え手順を実行するプログラムを作成して実行させることにより、誰でも容易に不揮発性メモリの中身を変更することができる。

【0005】

【発明が解決しようとする課題】この場合、不揮発性メモリの書き換え手順が正しい限りにおいてはその書き換えを阻止することは困難である。したがって、もし悪意を持つ人がそのような書き換えプログラムを作成してそれをインターネット等を通じてウィルスとして配布すると、そのウィルスを実行したPCの不揮発性メモリが不正に書き換えられてしまうという事態を招く危険がある。

【0006】本発明は上述の事情に鑑みてなされたものであり、ソフトウェアによる不揮発性記憶装置の不正な書き換えを阻止できるようにし、十分にセキュリティレベルの高い情報処理装置および不揮発性記憶装置の書き換え制御方法を提供することを目的とする。

【0007】

【課題を解決するための手段】上述の課題を解決するため、本発明は、不揮発性記憶装置の記憶内容を書き換え可能な情報処理装置であって、CPUと、前記不揮発性記憶装置の書き換えに必要な所定のハードウェアに対する、ソフトウェアからのアクセスにตอบสนองして、前記CPUに割り込み信号を発生する割り込み信号発生手段と、前記割り込み信号発生手段からの割り込み信号の発生を契機に前記CPUによって起動され、前記ソフトウェアによるアクセスが不当なものである場合、前記不揮発性記憶装置の書き換えを禁止する書き換え制御手段とを具備することを特徴とする。

【0008】この情報処理装置によれば、不揮発性記憶装置の書き換えに必要な所定のハードウェアに対する、ソフトウェアからのアクセスが発生すると、その時点でCPUに対して割り込み信号が自動的に発行される。そして、CPUの割り込み処理の中で書き換え制御手段が起動され、正当なアクセスである場合には不揮発性記憶

装置の書き換えがその時点で禁止される。このように、不揮発性記憶装置に対する書き換え処理手順が開始されたときに、専用の割り込み信号を発行して書き換え制御手段を起動するという仕組みを用いることにより、不揮発性記憶装置に対する不正な書き換えを阻止できるようになり、セキュリティレベルの向上を図ることが可能となる。

【0009】ソフトウェアによるアクセスが不当なものであるか否かの検出方法としては、例えば正当なソフトウェア（例えば、当該情報処理装置の製造メーカから配布されたソフトウェアなど）については書き換え処理とは直接関係しない所定の手順を事前に行うようにしておき、その手順が割り込み信号発生前にすでに行われているかどうかを調べるという方法を利用することができる。これにより、簡単でかつ正確に、ソフトウェアによるアクセスが正当なものであるか不当なものであるかを判定することができる。

【0010】また、書き換え制御手段の起動が封じられるのを防止するために、割り込み信号のマスクを禁止するためのマスク禁止手段を設けることが好ましい。

【0011】また、何らかの誤動作等によって不揮発性記憶装置の内容が誤って書き換えられてしまうという事態の発生を防止するために、不揮発性記憶装置の書き換え動作を行うアクセス制御手段にはライトプロテクト機能を設けておくことが好ましい。この場合、ソフトウェアによってライトプロテクト機能が解除されたことを契機に割り込み信号を発生し、そして不正なアクセスである場合には、再度ライトプロテクトの設定を行って不正な書き換えを阻止するという制御を利用することができる。

【0012】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図1には、本発明の一実施形態に係わるコンピュータシステムの構成が示されている。このコンピュータシステムはバッテリー駆動可能なノートブックタイプのパーソナルコンピュータ（PC）であり、このPC本体には、図示のように、プロセッサバス1、PCIバス2、ISAバス3、CPU11、ホスト-PCIブリッジ12、主メモリ13、表示コントローラ14、PCI-ISAブリッジ15、I/Oコントローラ16、通信コントローラ17、フラッシュBIOS-ROM18、およびEEPROM19などが設けられている。

【0013】CPU11は本PC全体の動作を制御するためのものであり、主メモリ13にロードされるオペレーティングシステム（OS）及びROM書き換えプログラムなどを実行する。ROM書き換えプログラムはフラッシュBIOS-ROM18を書き換えるためのソフトウェアである。このROM書き換えプログラムはOSの動作環境下で動作するように構成された一種のアプリケ

ーションプログラムであり、BIOS更新は、OSの動作環境下で実行することができる。

【0014】CPU11としては、システム管理割り込みSMI (SMI: System Management Interrupt) をサポートするものが利用される。即ち、CPU11はオペレーティングシステムやアプリケーション等を実行するための通常動作モードに加え、システム管理モード (SMM: System Management mode) と称されるシステム管理機能を実現するための動作モードを有している。

【0015】システム管理割り込み (SMI: System Management Interrupt) がCPU11に発行された時、CPU11の動作モードは、通常動作モード (リアルモード、プロテクトモード、または仮想86モード) から、SMMにスイッチされる。SMMでは、SMRAM131上のシステム管理プログラムが実行される。システム管理プログラムは、SMM-BIOSとしてフラッシュBIOS-ROM18に予め記憶されているものであり、システム起動時にフラッシュBIOS-ROM18からSMRAM131にコピーされる。本実施形態においては、システム管理プログラムの一つとして、不正なROM書き換え処理の実行を阻止するための割り込みハンドラが用意されている。この割り込みハンドラは、CPU11がSMMにスイッチしたときに実行される割り込み処理プログラムである。フラッシュBIOS-ROM18の書き換えに必要なPCI-ISAブリッジ15内の所定のハードウェアがソフトウェアによってアクセスされると、SMIがCPU11に発行され、これにより割り込みハンドラが起動される。システム起動中においては、SMRAM131にコピーされた割り込みハンドラの内容を書き換えることはできない。

【0016】ホスト-PCIブリッジ12は、CPUバス1とPCIバス2を双方向で接続するブリッジ装置であり、ここには主メモリ13をアクセス制御するためのメモリコントロール機能も内蔵されている。表示コントローラ14は本PCのディスプレイモニタとして使用されるLCDや外部CRTを制御する。

【0017】PCI-ISAブリッジ15は、PCIバス2とISAバス3とをつなぐブリッジであり、PCIバス2のバスマスタとして動作することができる。このPCI-ISAブリッジ15には、フラッシュBIOS-ROM18の書き換えに必要な動作を実行するための回路および前述のSMIを発生するための回路などが含まれている。

【0018】すなわち、PCI-ISAブリッジ15には、図示のように、フラッシュROM制御回路151、制御レジスタ152、SMI発生回路153、マスクレジスタ154、およびマスク禁止回路155などが設けられている。フラッシュROM制御回路151は、制御レジスタ152に設定されるソフトウェアからのコマン

ドに従ってフラッシュBIOS-ROM18のリード/消去/ライト動作を制御する。フラッシュBIOS-ROM18の書き換えは、フラッシュBIOS-ROM18の内容を一旦消去し、その後、必要なプログラムファイルをフラッシュBIOS-ROM18に書き込むことによって行われる。フラッシュROM制御回路151によるフラッシュBIOS-ROM18の消去/ライト動作は、制御レジスタ152内のライトプロテクトビットWPによって許可又は禁止される。ライトプロテクトビットWP="0"にセットすることにより、フラッシュROM制御回路151によるフラッシュBIOS-ROM18の消去およびライト動作の実行は禁止される。ROM書き換えプログラムによるROM書き換え手順の中には、ライトプロテクトビットWP="1"にして、ライトプロテクトを解除する処理が予め含まれている。

【0019】SMI発生回路153は、ライトプロテクトビットWPが"1"に書き換えられた時、それを要因としてSMI信号を発生する。マスクレジスタ154は、制御レジスタ152と同じく、CPU11がリード/ライト可能なレジスタであり、SMI信号の発生を許可または禁止するためのマスクデータを保持する。マスク禁止回路155はSMI信号のマスクを禁止するためのものであり、このマスク禁止回路155がソフトウェアによってアクティブ状態に設定されると、以降は、SMI信号の発生を禁止するためのマスクデータをマスクレジスタ154に書き込むことはできなくなる。

【0020】I/Oコントローラ16は、2次記憶として用いられるHDD161などのIDEデバイスを制御するためのバスマスタIDEコントローラを内蔵している。バスマスタIDEコントローラは、HDD161と主メモリ13との間のデータ転送のためにバスマスタとして動作することができる。また、I/Oコントローラ16は、DVDドライブやCD-ROMドライブを制御することもできる。

【0021】通信コントローラ17は例えば公衆網などを介してインターネット上の計算機と通信するためのものであり、モデムやISDNカードによって実現されている。BIOS更新を行う場合には、通信コントローラ17は、バージョンアップされた新たな更新BIOSファイルおよびROM書き換えプログラムをインターネット上のWEBサーバからダウンロードするために用いられる。ダウンロードされた更新BIOSファイルはHDD161に保存される。

【0022】フラッシュBIOS-ROM18は、前述したようにシステムBIOSを記憶するためのものであり、ソフトウェアによるBIOS更新を可能とするために電氣的に書き換え可能な不揮発性メモリであるフラッシュメモリ (フラッシュEEPROM) によって実現されている。システムBIOSは、PCのパワーオン時や再起動時に実行されるPOST (Power ON Se

If Test) ルーチン、各種 I/O デバイスを制御するためのデバイスドライバ群、システム環境を設定するための BIOS セットアップルーチンなどを体系化したものであり、PC 内のハードウェアを直接制御するために用いられる。また、このフラッシュ BIOS-ROM18 には、前述の SMM-BIOS も含まれている。

【0023】EEPROM19 には例えばパスワード等のセキュリティー管理に必要な情報が記憶されている。この EEPROM19 に対するリード/消去/ライト動作の制御もフラッシュ ROM 制御回路 151 によって行うことができる。

【0024】(フラッシュ ROM 書き換えに関するセキュリティー) 本実施形態のシステムにおいては、フラッシュ ROM 書き換えに関するセキュリティー機能として、以下の 5 つの機能が実装されている。

【0025】(1) 不適切なフラッシュ BIOS-ROM18 の書き換えに対しては、その書き換え手順の中の特定の処理により専用の割り込み (SMI) を発生させる仕組みを使い、割り込みハンドラの中で、フラッシュ ROM 書き換えを手順に従って実行してもフラッシュ ROM 書き換えが失敗するように書き換え処理を阻止する機能

(2) フラッシュ ROM 書き換え手順の中の特定の処理により発生する専用の割り込み (SMI) は、フラッシュ ROM 書き換えを行おうとしている時点ではマスクできないようにする機能

(3) フラッシュ ROM 書き換えを行おうとしている時点では、割り込みハンドラ自体を書き換えできないようにする機能

(4) 割り込みハンドラの中で実行するフラッシュ ROM 書き換え障害処理は、それに悪意の書き換え者が気が付いて排除しようとしても排除できないようにする機能

(5) 適正なフラッシュ ROM 書き換えに対しては、割り込みハンドラの中で、フラッシュ ROM 書き換え障害処理は行わず、正しくフラッシュ BIOS-ROM18 の書き換えを実行できるようにする機能

(フラッシュ ROM 書き換え制御処理 #1) 次に、図 2 のフローチャートを参照して、フラッシュ ROM 書き換え制御処理の手順について具体的に説明する。

【0026】ROM 書き換えプログラムは、一連の ROM 書き換え処理の中で、制御レジスタ 152 内のライトプロテクトビット WP を “1” に書き換えるハードウェアアクセスを実行し、フラッシュ BIOS-ROM18 のライトプロテクトを解除する (ステップ S101)。このとき、SMI 発生回路 153 から CPU11 に SMI 信号が発行される。この SMI 信号に応答して、実行中の ROM 書き換えプログラムが中断され、割り込みハンドラに制御が移される。

【0027】割り込みハンドラは、ROM 書き換えプロ

グラムによるアクセスが正当なものであるか否かの認証を行い (ステップ S201)、正当な書き換えのためのアクセスであるかどうかを判定する (ステップ S202)。この認証は、例えば、割り込まれたプログラムのプロセス名をチェックして当該 PC の製造メーカーから配布されたソフトウェアであるか否かを判定したり、あるいは正当なソフトウェアについては書き換え処理とは直接関係しない所定の手順をライトプロテクト解除前に事前に行うようにしておき、その手順が SMI 発生前にすでに行われているかどうかを調べる、ことなどによって行うことができる。

【0028】ROM 書き換えのための正当なアクセスであると判定された場合には、割り込みハンドラは、SMM からの復帰命令 (RSM) を実行して、ROM 書き換えプログラムに即座に制御を戻す。ROM 書き換えプログラムは、フラッシュ ROM 制御回路 151 にコマンドを発行し、フラッシュ BIOS-ROM18 の内容を書き換えるための処理 (フラッシュ BIOS-ROM18 の消去、書き込み) を実行する (ステップ S102)。これにより、フラッシュ BIOS-ROM18 の内容は正常に更新される。

【0029】一方、ROM 書き換えのための正当なアクセスではないと判定された場合には、割り込みハンドラは、制御レジスタ 152 内のライトプロテクトビット WP を “0” に書き換えるアクセスを実行し、フラッシュ BIOS-ROM18 のライトプロテクトを再設定する (ステップ S203)。この後、割り込みハンドラは、SMM からの復帰命令 (RSM) を実行して、ROM 書き換えプログラムに制御を戻す。ROM 書き換えプログラムは、フラッシュ BIOS-ROM18 の内容を書き換えるための処理 (フラッシュ BIOS-ROM18 の消去、書き込み) を実行するが (ステップ S102)、ライトプロテクトがなされているので、フラッシュ BIOS-ROM18 の内容を書き換えることはできない。つまり、不正な ROM 書き換えプログラムは、フラッシュ ROM 書き換えのための正しい処理を順次行っているにも関わらず、専用の割り込み発生とそれによる割り込みハンドラの処理により、狙い通りにフラッシュ ROM 書き換えを完遂することができない。

【0030】もし ROM 書き換えプログラムがライトプロテクトを再び解除したとしても、その場合には、再び割り込みハンドラによってライトプロテクトが再設定されるので、ROM 書き換えは失敗する。

【0031】なお、ROM 書き換えのための正当なアクセスではないと判定された場合、ライトプロテクトを再設定するだけでなく、不正な書き換えプログラムが実行されている旨の警告メッセージをディスプレイモニタに画面表示して、使用者に注意を促すようにしても良い。

【0032】(フラッシュ ROM 書き換え制御処理 #2) 次に、図 3 のフローチャートを参照して、フラッ

ROM書き換え制御処理の第2の手順について説明する。ここでは、予め決められた特定のレジスタに対するライトアクセスが行われているか否かによってプログラム認証が行われる。

【0033】正当なROM書き換えプログラムは、ステップS101のライトプロテクト解除処理を行う前に、予め決められた認証用のレジスタ内の所定ビット（認証フラグ）を“1”に設定する（ステップS111）。この認証用レジスタは本PC固有のスペシャルレジスタであり、そのI/Oアドレスおよびアクセス手順は秘密化されている。不正なROM書き換えプログラムは、認証フラグを“1”に設定せずに、ステップS101のライトプロテクト解除処理を行う。

【0034】ライトプロテクトが解除されたとき、SMI発生回路153からCPU11にSMI信号が発行される。このSMI信号にตอบสนองして、ROM書き換えプログラムから割り込みハンドラに制御が移される。割り込みハンドラは、認証フラグをチェックすることによって、ROM書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い（ステップS201）、正当なアクセスであるかどうかを判定する（ステップS202）。

【0035】認証フラグが“1”に設定されていれば、ROM書き換えのための正当なアクセスであると判定される。割り込みハンドラは、SMMからの復帰命令（RSM）を実行して、ROM書き換えプログラムに制御を戻す。ROM書き換えプログラムは、フラッシュBIOS-ROM18の内容を書き換えるための処理（フラッシュBIOS-ROM18の消去、書き込み）を実行する（ステップS102）。これにより、フラッシュBIOS-ROM18の内容は正常に更新される。

【0036】一方、認証フラグが“0”であれば、ROM書き換えのための不正アクセスであると判定される。この場合、割り込みハンドラは、制御レジスタ152内のライトプロテクトビットWPを“0”に書き換えるアクセスを実行し、フラッシュBIOS-ROM18のライトプロテクトを再設定する（ステップS203）。この後、割り込みハンドラは、SMMからの復帰命令（RSM）を実行して、ROM書き換えプログラムに制御を戻す。ROM書き換えプログラムは、フラッシュBIOS-ROM18の内容を書き換えるための処理（フラッシュBIOS-ROM18の消去、書き込み）を実行するが（ステップS102）、ライトプロテクトがなされているので、フラッシュBIOS-ROM18の内容を書き換えることはできない。

【0037】（フラッシュROM書き換え制御処理#3）次に、図4のフローチャートを参照して、フラッシュROM書き換え制御処理の第3の手順について説明する。ここでは、ライトプロテクトの再設定によって不正なフラッシュROM書き換えを阻止するのではなく、シ

ステムをシャットダウンすることによって阻止するという手法を用いる。

【0038】即ち、ライトプロテクトの解除によって起動される割り込みハンドラは、図3と同様の手法でROM書き換えプログラムによるアクセスが正当なものであるか否かの認証を行い（ステップS201）、正当なアクセスであるかどうかを判定する（ステップS202）。ROM書き換えのための正当なアクセスであると判定された場合は、割り込みハンドラは、SMMからの復帰命令（RSM）を実行するが、ROM書き換えのための不正アクセスであると判定された場合には、その時点でシステム電源を強制的にオフさせることなどによってシステムをシャットダウンする（ステップS203）。これにより、もはや不正なフラッシュROM書き換えは実行できなくなる。

【0039】なお、システムをシャットダウンする前にユーザに警告を発して、ライトプロテクトのみを行うか、安全性確保のためにシャットダウンを行うかをユーザに選択させるようにしても良い。

【0040】（SMIマスク禁止機能）次に、SMIのマスク禁止を行うための機能について説明する。上述のように、本実施形態のセキュリティ機能は、SMIを用いて実現されている。このため、SMIがマスクされるという妨害を受けると、セキュリティ機能が正常に働かなくなる。これを避けるため、システムBIOSのPOSTルーチンは、図5に示すように、POST処理の中でマスク禁止回路155を制御して、SMIのマスクを禁止する。

【0041】（SMI発生他の例）SMIの発生タイミングは、ライトプロテクト解除時ではなく、図6に示すように、例えばライトプロテクト解除後に行われるフラッシュROM制御回路151に対する最初の段階のI/Oアクセス時であってもよい。すなわち、フラッシュROM制御回路151に実際の消去動作を実行させるためにはソフトウェアによって制御レジスタ等に対する何らかのI/Oアクセスが逐次実行されることになるので、消去動作が実行される前の所定のI/Oアクセスをトリガに例えばI/OトラップSMIを発生し、これによって割り込みハンドラを起動させることもできる。

【0042】（割り込みハンドラの機能拡張）以上、不正なフラッシュROM書き換え処理を阻止するための制御処理について説明したが、本実施形態の仕組みは、フラッシュBIOS-ROM18の書き換えのみならず、重要なプログラムやデータが記録されている保護記憶領域、例えばEEPROM19、ハードディスク161内の特定記憶領域等の書き換えに対しても適用することができる。この様子を図7に示す。

【0043】コンピュータウィルスが保護記憶領域の書き換えに必要な一連の処理手順を開始すると、その特定の手順で行われるハードウェアへのアクセスにตอบสนองして

前述のSMIなどのハードウェア割り込み信号が発生され、これによって割り込みハンドラが起動される。割り込みハンドラは、プログラム認証を行い、不正な書き換えであればそれを阻止する処理を実行する。

【0044】以上説明したように、本実施形態においては、ROM書き換え用ハードウェアへの特定アクセスにより専用割り込みを発生させる仕組みを用いることにより、セキュリティ制御を適正な時点で実行させることができ、十分にセキュリティレベルの高いシステムを実現することが可能となる。なお、SMIに限らず、他のハードウェア割り込みを利用し、OS上で動作するユーティリティなどを割り込みハンドラとして起動させるようにしてもよい。

【0045】また、本発明は、上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【0046】

【発明の効果】以上説明したように、本発明によれば、ソフトウェアによる不揮発性記憶装置の不正な書き換えを阻止できるようになり、十分にセキュリティレベルを確保することが可能となる。

ムの構成を示すブロック図。

【図2】同実施形態のシステムで使用するフラッシュROM書き換え制御処理の手順を示すフローチャート。

【図3】同実施形態のシステムで使用するフラッシュROM書き換え制御処理の第2の手順を示すフローチャート。

【図4】同実施形態のシステムで使用するフラッシュROM書き換え制御処理の第2の手順を示すフローチャート。

【図5】同実施形態のシステムで使用するPOST処理の手順を示すフローチャート。

【図6】同実施形態のシステムで使用する割り込みハンドラ起動処理の他の例を示す図。

【図7】同実施形態のシステムで使用する割り込みハンドラの機能拡張の一例を説明するための図。

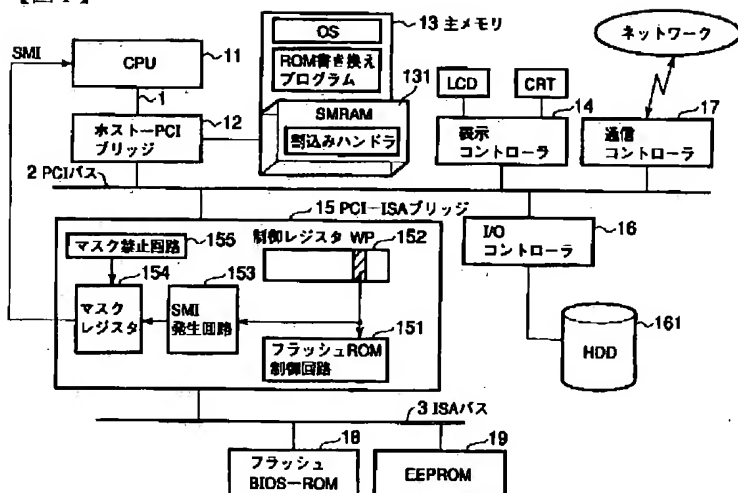
【符号の説明】

- 11…CPU
- 12…ホスト-PCIブリッジ
- 13…主メモリ
- 15…PCI-ISAブリッジ
- 16…I/Oコントローラ
- 17…通信コントローラ
- 18…フラッシュBIOS-ROM
- 19…EEPROM
- 131…SMRAM
- 151…フラッシュROM制御回路
- 152…制御レジスタ
- 153…SMI発生回路
- 154…マスクレジスタ
- 155…マスク禁止回路

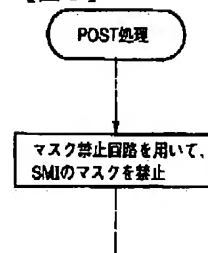
【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンピュータシステム

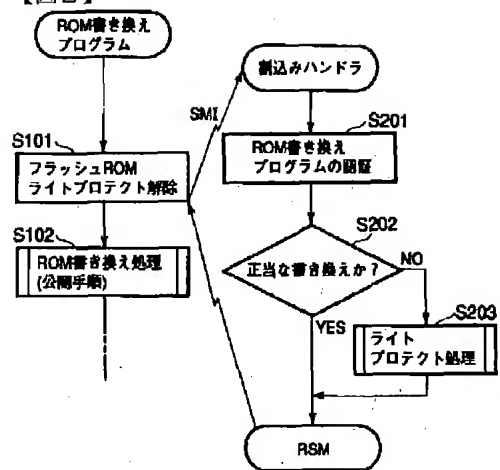
【図1】



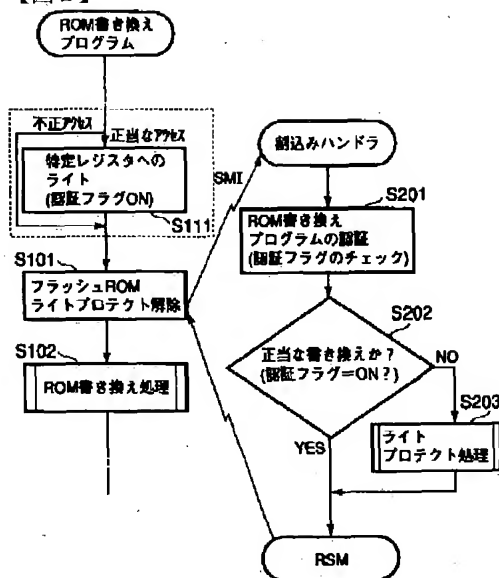
【図5】



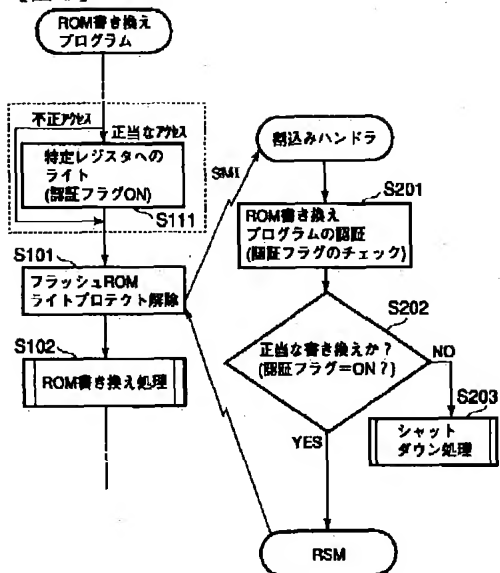
【図2】



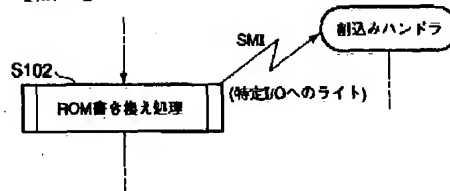
【図3】



【図4】



【図6】



【図7】

